Licence 3 – 4TTI603U Université de Bordeaux
2024/2025

Feuille 3 : RSA

Exercice 1. Chiffrement RSA

1. Soit $n = pq$, où p et q sont des nombres premiers distincts. Le système RSA chiffre $m \in \mathbb{Z}/n\mathbb{Z}$ en $m^e \in \mathbb{Z}/n\mathbb{Z}$, où e est inversible modulo $\varphi(n)$. Puis on déchiffre $c \in \mathbb{Z}/n\mathbb{Z}$ en calculant $c^d \in \mathbb{Z}/n\mathbb{Z}$, où d est l'inverse de e modulo $\varphi(n)$.
   (a) Quelle est la clé publique ? La clé privée ?
   (b) Pourquoi vaut-il mieux prendre m dans $(\mathbb{Z}/n\mathbb{Z})^\times$? Soit x pris au hasard avec probabilité uniforme dans $\mathbb{Z}/n\mathbb{Z}$. Quelle est la probabilité pour que $x \in (\mathbb{Z}/n\mathbb{Z})^\times$?
   (c) Montrer que le système est correct, c'est-à-dire que si c est un chiffré de m alors le déchiffrement de c redonne bien m (même si $m \notin (\mathbb{Z}/n\mathbb{Z})^\times$).
   (d) La composée de deux chiffrements RSA de même module n est-elle un chiffrement RSA ?
   (e) Dans cette question on fixe p et q deux nombres premiers distincts. Combien a-t-on de choix pour la clé publique ?
2. Dans cette question on souhaite implémenter un système RSA avec $n = 221$.
   (a) Calculer $\varphi(n)$.
   (b) Vérifier que l'on peut choisir 7 comme exposant de chiffrement.
   (c) Chiffrer le message $m = 3$ pour cet exposant.
   (d) Calculer la clé privée.
   (e) Déchiffrer le message $c = 198$.

Exercice 2. Déchiffrement de RSA

Dans cette exercice, on montre comment on peut accélérer le déchiffrement du système RSA en utilisant le théorème des restes chinois. Soit $n = pq$ produit de deux nombres premiers distincts et $d \in \mathbb{N}$ premier avec $\varphi(n)$. On s'intéresse au calcul du déchiffrement $c^d \pmod{n}$.

1. On pose $m_p \equiv c^d \pmod{p}$, $m_q \equiv c^d \pmod{q}$, $d_p = d \mod (p-1)$ et $d_q = d \mod (q-1)$. Montrer que $m_p \equiv c^{d_p} \pmod{p}$ et $m_q \equiv c^{d_q} \pmod{q}$.
2. Soit le système dans $\mathbb{Z}/n\mathbb{Z}$:
$$\begin{cases} m \equiv m_p \pmod{p} \\ m \equiv m_q \pmod{q} \end{cases}$$
   Justifier que si m est solution du système ci dessus alors $m \equiv c^d \pmod{n}$.
3. Comparer la complexité de cet algorithme de déchiffrement avec celle de l'algorithme usuel.
4. En utilisant cette méthode déchiffrer le message $c = 198$ pour $n = 221$ et $d = 67$.

Exercice 3. Dans RSA, connaître $\varphi(n)$ est équivalent à connaître p et q

Soit $n = pq$ produit de deux nombres premiers distincts.

1. Exprimer pq et $p+q$ en fonction de n et $\varphi(n)$. En déduire une méthode pour obtenir p et q lorsque l'on connait n et $\varphi(n)$.
2. Si $n = 17063$ et $\varphi(n) = 16800$, calculer p et q.

Exercice 4. Une attaque sur RSA : petit exposant public commun

On suppose que k personnes $B_1, \ldots, B_k$ ont pour exposant public RSA $e = 3$ avec des modules respectifs n_i, $1 \leq i \leq k$.

1. Pourquoi est-il raisonnable de supposer que les n_i, $1 \leq i \leq k$ sont deux à deux premiers entre eux ?
2. Alice envoie les chiffrés d'un même message m à tous les B_i. Montrer qu'un attaquant peut déterminer m^3 modulo $P := \prod_{i=1}^{k} n_i$; en déduire qu'il peut calculer m si $P > m^3$.
3. Quelle est la valeur minimale de k qui permet de toujours faire cette attaque ?

Exercice 5. Une attaque sur RSA : module commun

Bob et Catherine ont choisi le même module RSA n. Leurs exposants publics e_B et e_C sont distincts.

1. Expliquer pourquoi Bob peut déchiffrer les messages reçus par Catherine et réciproquement.
2. On suppose que e_B et e_C sont premiers entre eux et qu'Alice envoie les chiffrés d'un même message m à Bob et à Catherine. Expliquer comment l'attaquant Oscar peut obtenir m.
3. Application : Bob a la clé publique $(221, 11)$ et Catherine la clé $(221, 7)$. Oscar intercepte les chiffrés 210 et 58 à destinations respectives de Bob et Catherine. Retrouver le message m.

Exercice 6. Module RSA avec deux facteurs proches

Supposons que n soit un entier produit de deux nombres premiers p et q, $p > q$. On suppose que p et q sont proches, c'est à dire que $\epsilon := p - q$ est petit. On pose $t = \frac{p+q}{2}$ et $s = \frac{p-q}{2}$.

1. Montrer que $n = t^2 - s^2$.
2. Quelle est la taille de s ? Comparer t et $\sqrt{n}$.
3. Montrer comment utiliser cela pour écrire un algorithme (de Fermat) factorisant n.
4. Application : factoriser 11598781.
5. Déterminer le nombre d'itérations de l'algorithme en fonction de p et de n. Que se passe-t-il si $p - \sqrt{n} < \sqrt[4]{4n}$?